UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

A 1997 FORD EXPEDITION, BLACK IN COLOR BEARING OHIO LICENSE #GSH2644 (SUBJECT VEHICLE #1) LOCATED AT: 1662 FENTON BUSINESS PARK CT., FENTON, MO 63026, LOCATED IN THE EASTERN DISTRICT OF MISSOURI.

Case No. 4:24-MJ-9074 RHH

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Jeremy Bluto, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

Title 18, United States Code, Sections 2251 (production of child pornography); Section 2252A (receipt, distribution, and possession of child pornography); Section 2422 (online enticement and solicitation of sex with a minor)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Applicant's signature

Jeremy Bluto, Special Agent

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date: 02/27/2024

Judge's signature

City and state: St. Louis, MO

Honorable Rodney H. Holmes, U.S. Magistrate Judge

Printed name and title

AUSA: Nathan Chapman

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF A 1997 FORD EXPEDITION, BLACK IN COLOR BEARING OHIO LICENSE #GSH2644 (**SUBJECT VEHICLE #1**) LOCATED AT: 1662 FENTON BUSINESS PARK CT., FENTON, MO 63026, LOCATED IN THE EASTERN DISTRICT OF MISSOURI.	No. 4:24-MJ-9074 RHH SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jeremy Bluto, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1662 Fenton Business Park Ct., Room #227, Fenton, MO 63026, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent (SA) with Immigration and Customs Enforcement / Homeland Security Investigations (HSI), Kansas City, Missouri, Principal Field Office, and have been so employed since April 25, 2010. I am currently assigned as a criminal investigator for HSI and a member of the Southwest Missouri Cyber Crimes Task Force (SMCCTF). Prior to my current position, I was employed with U.S. Customs and Border Protection, Office of Border Patrol, as a Border Patrol Agent and a Supervisory Border Patrol agent for five years, and a Deputy Sheriff with the Taney County, Missouri, Sheriff's Department for three years. Prior to my employment in Missouri, I attended California State University, Fullerton, and received a bachelor's degree in Criminal Justice.

3. As part of this affiant's duties with HSI, I investigate criminal violations relating to child exploitation, child pornography, and coercion and enticement, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422. I have received training in the areas of child pornography, child exploitation, coercion and enticement, and human/sex trafficking.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from local and federal law enforcement and witnesses.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2251, 2252A, and 2422 (the "SUBJECT OFFENSES") have been committed by Travis SHERWOOD. Section 2251 criminalizes the production of child pornography. Section 2252A criminalizes, among other things, the receipt, distribution, and possession of child pornography. Section 2422 criminalizes the online enticement and solicitation of sex with a minor. There is also probable cause to search the premises described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

VEHICLES TO BE SEARCHED

6. The vehicle to be searched is a 1997 Ford Expedition, black in color, bearing Ohio license #GSH2644 (**SUBJECT VEHICLE #1**). Both vehicles are registered in Ohio and return to TRAVIS SHERWOOD, who currently resides at 1662 FENTON BUSINESS PARK CT., ROOM #227, FENTON, MO 63026. The **SUBJECT VEHICLES** are further described in the Attachment A, and the accompanying photographs of the vehicles.

DEFINITIONS

7. The following terms have the indicated meaning in this affidavit:

a. The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device. 18 U.S.C. § 1030(e). The term computer included cellular telephones.

b. The term "minor" means any individual under the age of 18 years. 18 U.S.C. § 2256(1).

c. "Sexually explicit conduct" means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 U.S.C. § 2256(2)(A).

d. "Visual depiction" includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 U.S.C. § 2256(5).

e. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or (C) such visual depiction has been created, adapted, or modified to

appear that an identifiable minor is engaging in sexually explicit conduct. 18 U.S.C. § 2256(8)(A) or (C).

f. "Identifiable minor" means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 U.S.C. § 2256(9).

g. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game counsels and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic

notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

m. "Wireless telephone or mobile telephone, or cellular telephone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

COMPUTERS AND CHILD PORNOGRAPHY COLLECTORS

8. From my own training and experience in the area of Internet and electronic-facilitated child exploitation investigations, and through consultation with other knowledgeable law enforcement officials, I know the following to be true.

9. Computers connected to the Internet identify each other by an IP address. An IP address can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

10. The information contained in this section is based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions.

11. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based/ subscription-based Web sites to conduct business, allowing them to remain relatively anonymous. Child pornography is also traded through chat rooms and file sharing software.

12. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the

computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

13. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

14. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both

the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the Web sites and images accessed by the recipient.

15. The computer's capability to store images in digital form makes it an ideal repository for child pornography. Hard drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

16. Based upon my training and experience, I have found that child pornography distributors/collectors:

a. receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity;

b. collect sexually explicit or suggestive materials (hard-core and soft-core pornography, whether of adults and/or of children) in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. Further, they commonly use this type of sexually explicit material to lower the inhibitions of

children they are attempting to seduce, to arouse the selected child partner, and to demonstrate the desired sexual acts;

c. almost always possess and maintain their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, child erotica,1 etc.) in the privacy and security of their homes or some other secure location. Child pornography distributors/collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. Additionally, there is a probability that suspects may maintain a portion of his collection of child pornography in a hard form such as pictures printed from computer files;

d. often correspond and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

e. prefer not to be without their child pornography and/or child erotica for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world;

f. maintain their collections in a safe, secure environment, such as his computer and surrounding area, because this material is illegal, difficult to obtain, and difficult to replace. These collections are maintained indefinitely and are kept close by, usually at their residence, to enable the collector to view his collection, which he values highly; and

g. often correspond and/or meet others to share information and materials; rarely destroy correspondence from other preferential child pornographers; conceal such correspondence as they do their sexually explicit material and often maintain lists of names, addresses and telephone numbers of individuals with whom they have been in contact and who share the same interest in child pornography.

PROBABLE CAUSE

17. HSI received a CyberTipline Report (CTR) 176545299 from the Christian County, Missouri, Sheriff's Office (CCSO) to NCMEC (National Center for Missing and Exploited Children) on October 23, 2023. Your affiant has reviewed this report. CCSO submitted the CTR to NCMEC after determining they would be unable to file state charges based on the age of the victim. By way of background, United States law, Title 18, United States Code §2258A, identifies NCMEC as the central repository for these reports and further permits NCMEC to share this information with law enforcement. NCMEC categorized this report as ONLINE ENTICEMENT – PRE-TRAVEL.

18. The above referenced CTR described a report (CCSO # SO-23-01262) made by a resident in Christian County, Missouri, indicating his 15-year-old daughter (Hereafter MV1) was talking to an adult male subject through an application called Chatib. The adult male was identified as Travis SHERWOOD and had requested and received nude photographs of MV1.

19. On October 26, 2023, this affiant contacted CCSO Detective (Det.) Sarah Spurlock. Det. Spurlock stated CCSO had taken the initial report on September 3, 2023. Det. Spurlock stated two cell phones being used by MV1 were surrendered by her parents who had signed consent forms permitting a forensic examination of the cell phones. On the same date, this affiant collected the two cell phones and all CCSO reports related to the incident.

20. This affiant reviewed CCSO Report #SO-2023-01262. MV1's mother stated she had discovered a chat between MV1 and a suspect using phone number (614) 852-8050 who identified himself as "Travis" on MV1's primary cell phone. The CCSO responding deputy was given permission to look through the chat and discovered a nude photograph of MV1 was sent to (614) 852-8050 on August 25, 2023, at 4:08 AM.

21. On November 2, 2023, HSI SA Charles Rogener, a trained Cellebrite examiner, conducted a mobile device extraction on MV1's primary cell phone, a Samsung Z Flip4 with IMEI 354352150271804. SA Rogener provided this affiant with a copy of the extraction.

22. On November 6, 2023, HSI SA Rogener conducted a mobile device extraction on MV1's secondary cell phone, a Samsung Note 9, model SM-N950U. SA Rogener provided this affiant with a copy of the extraction.

23. This affiant reviewed the cell phone extractions and discovered a text/chat conversation on MV1's primary cell phone between MV1 and a subject utilizing phone number (614) 852-8050. Within the chat conversation, the subject using phone number (614) 852-8050 identifies himself as "Travis" and later says his last name is "SHERWOOD". The text/chat begins on August 25, 2023, at approximately 1:30 am Central Daylight Time (CDT) and ends on August 26, 2023, at approximately 12:19 pm CDT.

24. On August 25, 2023, at approximately 1:42 am CDT, (614) 852-8050 sends a photograph to MV1 depicting a white male, approximately 35-40 year of age, with brown hair and a brown beard, wearing eyeglasses and a black tank top, with a brown and black kitten sitting on his shoulder.

25. This affiant was able to locate an Ohio driver license issued to a Travis D. SHERWOOD, date of birth: March 26, 1983. The driver license photo depicted a white male with

brown hair and a brown beard, wearing eyeglasses. This affiant compared the photograph sent to MV1 with the driver license photo and believes they are the same person.

26. On August 25, 2023, at approximately 2:04 am CDT, SHERWOOD and MV1 have the following text/chat exchange:

a. SHERWOOD: Can I See? Pretty Please?

b. MV1: What do you wanna see, just another selfie?

c. SHERWOOD: If you fell alright with nit. It's entirely up to you.

d. MV1: Okay

i. The photograph sent by MV1 had been deleted from the chat, however, this affiant, discovered a selfie of MV1 recovered from the deleted files in the phone. The photo was created on August 25, 2023, at approximately 2:10 am CDT. The photo depicted MV1 wearing a dark colored, hooded sweatshirt.

e. SHERWOOD: How'd I get so lucky to find you:

f. SHERWOOD: Surprise eye candy

i. SHERWOOD sent a selfie style photograph of himself wearing a black tank top flexing in a mirror.

g. SHERWOOD: For my Olivia.

i. "Olivia" is an alias used my MV1.

h. MV1: Thank you!!

27. As the conversation continues, SHERWOOD directs the conversation toward sex and asks MV1 if she thinks she is ready for sex. On August 25, 2023, at approximately 3:19 am CDT, SHERWOOD and MV1 have the following text/chat exchange:

a. SHERWOOD: Mmm imagine me holding you right now

b. MV1: I want you too

c. SHERWOOD: I hope I'm not turning you on too much

d. MV1: Just a tad but you're fine

e. SHERWOOD: Me now 😉

i. SHERWOOD sends a photograph that appears to be of a pair of yellow plaid-colored boxers with black pants pulled down to show the boxers. There is a bulge in the middle of the boxers, presumably from an erect penis.

f. MV1: Mmm

28. As the conversation continues, SHERWOOD and MV1 begin to role play about being intimate with each other. On August 25, 2023, at approximately 3:46 am CDT, SHERWOOD and MV1 have the following text/chat exchange:

a. SHERWOOD: *one finger slips under them* mmm wish I could see you in just your panties

b. MV1: I'll give you a picture if you want

c. SHERWOOD: 😊 Surprise me

d. MV1: Okay

i. The photograph sent by MV1 had been deleted from the chat, however, this affiant, discovered a photograph recovered from the deleted files in the phone. The photo was created on August 25, 2023, at approximately 2:10 am CDT. The photo depicted a female

seated with her legs spread open. The female is wearing a black bra and red panties with a black, paisley print.

e. SHERWOOD: Mmm sexy *kisses lower, tracing over your panties*

f. SHERWOOD: You look so good in red and black

g. MV1: Mmm, thank you

29. The conversation continues and on August 25, 2023, at approximately 4:00 am CDT, SHERWOOD and MV1 have the following text/chat exchange:

a. SHERWOOD: Right now, I am so tempted to slip that bra off of you.

b. MV1: Mmm, come do it

c. SHERWOOD: *undoes your bra, sliding it down, your beautiful b cups on display for me*

d. MV1: Mmm

e. SHERWOOD: What would you say to one more like that with you wearing nothing at all *traces over your sensitive nipples*

f. MV1: Mm, one more picture?

g. SHERWOOD: If you're okay with it, it's your call love

h. MV1: Yeah, I can do it

i. SHERWOOD: You're sure about it? Baby, you can tell me no and I won't be upset

j. MV1: Nono, I'm fine, I promise

k. SHERWOOD: Okay, it's entirely your choice 😊

l. MV1: Thank you

i. The photograph sent by MV1 had been deleted from the chat, however, this affiant, discovered two photographs recovered from the deleted files in the phone. The first photo was created on August 25, 2023, at approximately 4:07 am CDT. The photo depicted a female seated with her legs spread open, naked, with her bare breasts and vagina visible. The photograph was slightly blurry. The second photo was created on August 25, 2023, at approximately 4:08 am CDT and depicted the same female in the same pose, but this photo was not blurry.

m. SHERWOOD: Beautiful

n. MV1: Is it okay?

o. SHERWOOD: You are beyond stunning.

p. MV1: Thank you

q. SHERWOOD: If you were here right now, I would take your virginity and make you mine forever

r. MV1: Mmm, I wish you could

30. On October 27, 2023, this affiant determined phone number (614) 852-8050 was assigned to T-Mobile. On the same date, a Department of Homeland Security (DHS) Summons was served on T-Mobile requesting subscriber information for phone number (614) 852-8050. On November 6, 2023, T-Mobile provided a return indicating the phone number was subcontracted to Tracfone Wireless, Inc.

31. On November 6, 2023, a DHS Summons was served on Tracfone Wireless, Inc., requesting subscriber information for phone number (614) 852-8050. On December 6, 2023, Tracfone Wireless, Inc., responded and provided the following subscriber information:

a. First Name: NoReal

b. Last Name: NoReal

c. Address: 429 n colombus st. pat. 2

d. City: Lancaster

e. State: OH

f. Zip: 43130

g. Email: cd9sherwood@yahoo.com

32. On February 8, 2024, a DHS Summons was served on Yahoo Inc. requesting subscriber information and IP logs connected to the account cd9sherwood@yahoo.com. On February 9, 2024, Yahoo Inc. responded and provided the following subscriber information:

a. Other Identities: cd9asherwood

b. GUID: RB46VR7R32HZB3NGZNZI6OD6GI

c. Mail Name: cd9asherwood@yahoo.com

d. Account Status: active

e. Registration IP Address: 68.250.187.190

f. Registration Date: 2006-11-07T15:14:11.000Z

g. Full Name: Travis Sherwood

h. Address: 1301 Sylvan Ave.

i. City: Lancaster

j. State, territory, or province: OH

k. Country: US

l. Zip/Postal Code: 43130

m. Phone: 740-654-8662

n. Time Zone: ET

o. Recovery Emails: fc3ssherwood@gmail.com Verified on: 2021-02-02T15:55:46Z

33. Yahoo Inc. also provided an IP connection log covering the period from February 7, 2023, to February 8, 2024. IP addresses 68.191.194.123 appeared more than any other IP address on the report. IP address 68.191.194.123 was used on August 25, 2023 and August 26, 2023, the time period when SHERWOOD was communicating with MV1. IP address 68.191.194.123 last accessed the account on February 8, 2024.

34. IP address 68.191.194.123 is registered to Charter Communications, Inc. On February 9, 2024, a DHS Summons was issued to Charter Communications, Inc., requesting subscriber information for IP address 68.191.194.123 on August 25, 2023 at 21:07:42 UTC. On February 15, 2024, Charter Communications, Inc. responded and provided the following subscriber information:

a. Subscriber Name: THW 1662

b. Service Address: 1662 Fenton Business Park Ct., ST SB, Fenton, MO 63026-2990

c. Billing Address: PO Box 1147, Holland, OH 43528

d. User Name or Features:

i. ACCOUNTING@YOURTIMECLOCKSOLUTION.COM

BBARSHA@YOURTIMECLOCKSOLUTION.COM

35. This affiant went to the website yourtimeclocksolution.com and discovered the company provides internet services, and other services, to third party companies.

36. This affiant learned that 1662 Fenton Business Park Ct., ST SB, Fenton, MO 63026-2990 is the address of Extended Stay America Suites – St. Louis – Fenton.

37. On February 21, 2024, HSI SA's and Task Force Officers (TFO's) conducted surveillance at the Extended Stay America Suites, 1662 Fenton Business Park Ct., ST SB, Fenton, MO 63026-2990. The Extended Stay America consists of two buildings with a shared parking lot. The main building with the office is located on the east side of the parking lot and the second building is located on the west side of the parking lot.

38. Agents observed a black Ford Expedition bearing Ohio license #GSH2644 (**SUBJECT VEHICLE #1**) and a silver BMW bearing Ohio license #HOP269 (**SUBJECT VEHICLE #2**) in the parking lot. The **SUBJECT VEHICLES** are both registered to Travis SHERWOOD, 3138 E. 5th Ave., Columbus, OH 43219.

39. Travis SHERWOOD is the subject of this investigation. Based on this affiant's training and experience, people who live in hotels are transient in nature. Hotel rooms have limited storage space and vehicles are often used as a secondary storage location. The Yahoo account associated with Travis SHERWOOD has accessed internet though Wi-Fi service provided by the hotel. Wireless internet signals vary in strength, but often extend beyond the building into adjacent parking areas.

40. On February 21, 2024, at approximately 12:04 pm, CST, agents observed SHERWOOD, who was identified based on his driver license photo and photographs sent by him to MV1, exit the southern door of the west building and walk over to **SUBJECT VEHICLE #1**.

SHERWOOD was working on the vehicle for approximately 27 minutes at which time he re-entered the west building.

41. SHERWOOD was observed by agents, using a key card to enter room #227, on the second floor of the west building.

42. On February 21, 2024, MV1 was interviewed by an HSI Forensic Interview Specialist (FIS). The FIS spoke to MV1 who stated, in August 2023, she had engaged in several conversations and sent sexually explicit photographs to several people online. MV1 was shown sections of the text/chat messages she exchanged with SHERWOOD. MV1 read the sections and did not remember it based off the chats. MV1 was shown a photograph SHERWOOD and a cat that he sent to her during the conversation. MV1 recognized him as someone she sent pictures to but did not remember his name or how many pictures she sent. MV1 said she remembered he spoke Japanese.

a. During the text/chat SHERWOOD told MV1 about translating a service manual for a Mazda RX7 from Japanese to English, and sent her a video of him speaking Japanese to MV1.

43. MV1 positively identified herself in a selfie sent to SHERWOOD and described in paragraph 26(d)(i) above.

44. MV1 said she did not want to look at any sexually explicit photographs she may have sent to SHERWOOD or any other person. MV1 did agree to look at the photograph of a female in a bra and panties described in paragraph 28(d)(i) above. MV1 positively identified herself in the photograph. Although the photograph did not show her head and face, she recognized the panties and also said she recognized her moles. She stated has two moles on the right-middle side of her abdomen and a mole on her left side.

45. This affiant reviewed the photograph of the female, seated with her legs spread and naked described in paragraph 29(l)(i) and found the room details, color and length of the victim's hair, and size and location of MV1's moles, and determined the photograph was of MV1. Based on MV1's age and this affiants training and experience, this image depicts child pornography.

SEIZURE OF EQUIPMENT AND DATA

46. As detailed in the Computers and Child Pornography section of this affidavit, computers and the Internet make it easy to share information between devices. Additionally, based on training and experience, your Affiant is aware collectors of child pornography often transfer and store child pornography on multiple devices and media.

47. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

48. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.

49. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

50. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such-- or whether is serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readable, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is

ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

51. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

52. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices, in order for a qualified computer

expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

53. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

SEARCH METHODOLOGY TO BE EMPLOYED

54. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer system(s) and computer hardware to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);

b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

USE OF BIOMETRIC FEATURES TO UNLOCK ELECTRONIC DEVICES

55. The warrant I am applying for would permit law enforcement to compel Travis SHERWOOD to unlock a device subject to seizure pursuant to this warrant that is his possession or for which law enforcement otherwise has a reasonable basis to believe is used by him using the device's biometric features. I seek this authority based on the following:

56. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

a. I have probable cause to believe that one or more of the electronic devices in the **SUBJECT VEHICLES** are likely to offer its user the ability to use biometric features to unlock the device(s). Your affiant knows that many smart phones use fingerprint sensor technology and facial recognition to unlock the phone.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a

feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition

features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

57. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

58. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has

remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

59. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and the device is in Travis SHERWOOD's possession or law enforcement otherwise has a reasonable basis to believe is used by Travis SHERWOOD, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of Travis SHERWOOD, to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of Travis SHERWOOD, and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of Travis SHERWOOD, and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

CONCLUSION

60. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to search the vehicles described in Attachment A and any computers, computer hardware, computer media, digital tablets, wireless telephones and data storage devices therein, and seize such items for search for the items described in Attachment B.

61. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their

premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

JEREMY BLUTO
Special Agent
Homeland Security Investigations

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 27th day of February 2024.

HONORABLE RODNEY H. HOLMES
United States Magistrate Judge

SW 4:24-MJ-9074 RHH

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The vehicle to be searched are a 1997 Ford Expedition, black in color, bearing Ohio license #GSH2644. The vehicle is registered in Ohio and return to TRAVIS SHERWOOD, who currently resides at 1662 FENTON BUSINESS PARK CT., ROOM #227, FENTON, MO 63026.

SW 4:24-MJ-9074 RHH

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

All records, items, and information relating to violations of Title 18, United States Code, Sections 2251, 2252A, and 2422, that constitute fruits, evidence and instrumentalities of those violations involving including:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt, or storage of the same, including but not limited to:

a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);

b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer and cell phone passwords and other data security devices designed to restrict access to or hide computer or cell phone software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, materials, emails, communications and/or internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of sexual exploitation of minors, child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received and

4. Any and all records, documents, records, materials, invoices, notes and/or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

5. Documents, records and/or materials regarding the ownership and/or possession of the SUBJECT PREMISES.

6. During the course of the search, photographs and/or videos of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

7. During the execution of the search of the SUBJECT PREMISES, law enforcement personnel are also specifically authorized to obtain from **TRAVIS SHERWOOD**, if he is on the SUBJECT PREMISES at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any electronic device, such as, but not limited to computers, computer hardware, cell phones, and tablets, requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

(a) any of the Device(s) found at the SUBJECT PREMISES

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the electronic device(s)'s, which include, but are not limited to, computers, computer hardware, cell phones, and tablets, security features in order to search the contents as authorized by this warrant.

8. The terms "records," "documents," and "materials," as used in Attachment B, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, DVDs, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), thumb drives, flash drives, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

As used in Attachment B, the term computer includes cellular telephones/smartphones.